Supplementary Reference: 545
File Name: 545saf_040600
Last Revised: 04/07/2000

Synopsis of Security Practices for Users

This brief synopsis of security practices for users of unclassified automated information systems (AISs) is provided to assist in understanding guidance provided in ADS 545. This document is not all-inclusive; for additional assistance on security matters relating to processing unclassified data, contact your Information System Security Officer (ISSO.)

1. Read, understand and implement/execute:

    a. AIS security policies.

    {Automated Directives System (ADS), State Department Guidance etc.}

    b. AIS security forms.

    {Authorized Access List, Fax Cover Sheet, USAID Computer System Access & Termination Request, USAID Sensitive Data Nondisclosure Agreement, USAID Unclassified Automated Information Systems Access Request Acknowledgement, Visitor's Log etc.}

2. Make your password(s) unique and hard to guess or "crack."

3. Use current anti-virus software to scan data (especially new data.)

4. Log off your workstation when you leave your area.

5. Back up your files.

6. Follow the Agency's rules of behavior; some user rules of behavior are:

    a. Access only data you are authorized to use:

        (1) Don't use or change any account, file, record, or application (software program) not required to perform your official duties or officially authorized activities.

        (2) Don't access someone else's account or files without formal authorization from your supervisor.

        (3) Remember not to access or disclose sensitive or personal data unless necessary to perform official duties.

b. Work with others to administer necessary safeguards and controls:

(1) Cooperate with inspectors and evaluators.

(2) Assist in completion of the automated information system certification/approval to operate process, and contingency planning for information resources.

(3) Participate in AIS security training and awareness programs.

c. Be careful with AIS resources (software, hardware, communications means, etc.)

(1) Don't move equipment or exchange components without authorization from the appropriate Information Technology (IT) Systems support element.

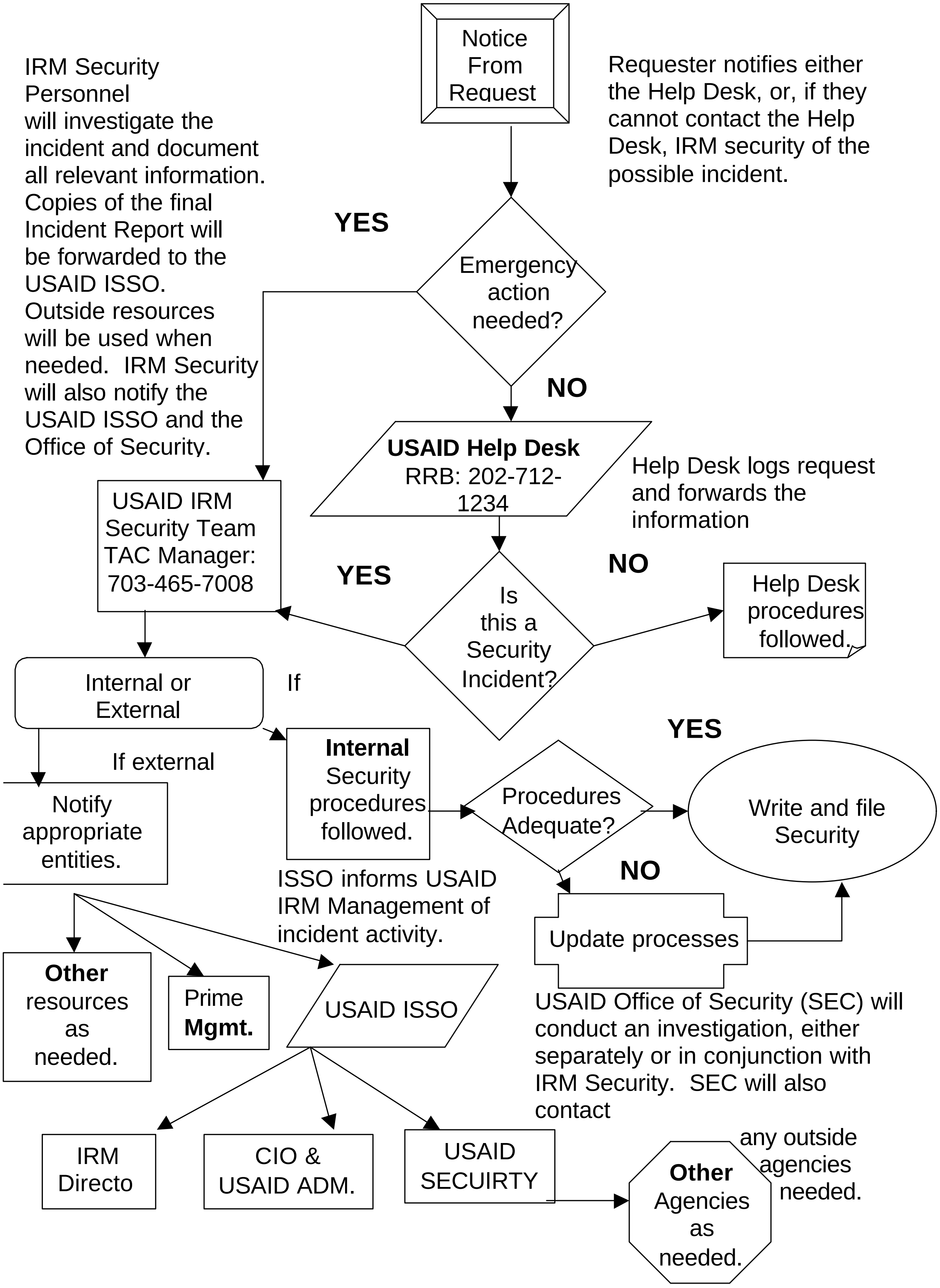
(2) Protect AIS resources from physical hazards such as liquids, food, smoke, staples, paper clips, etc.

(3) Don't install or use unauthorized software on AIS.

(4) Comply with all software licensing agreements; don't violate Federal copyright laws.

(5) Don't overload systems with extraneous matter (e.g., keep email attachments small, avoid excessive graphics on web pages, limit length of facsimile transmissions etc.)

7. Report AIS security incidents (see diagram on the next page.)


Notice From Request
Emergency action needed?
YES
NO
USAID Help Desk RRB: 202-712-1234
USAID IRM Security Team TAC Manager: 703-465-7008
YES
NO
Is this a Security Incident?
Help Desk procedures followed.
Internal or External
If
If external
Internal Security procedures followed.
Procedures Adequate?
YES
Write and file Security
NO
Update processes
Notify appropriate entities.
Other resources as needed.
Prime Mgmt.
USAID ISSO
IRM Directo
CIO & USAID ADM.
USAID SECUIRTY
Other Agencies as needed.

Requester notifies either the Help Desk, or, if they cannot contact the Help Desk, IRM security of the possible incident.

IRM Security Personnel will investigate the incident and document all relevant information. Copies of the final Incident Report will be forwarded to the USAID ISSO. Outside resources will be used when needed. IRM Security will also notify the USAID ISSO and the Office of Security.

Help Desk logs request and forwards the information

ISSO informs USAID IRM Management of incident activity.

USAID Office of Security (SEC) will conduct an investigation, either separately or in conjunction with IRM Security. SEC will also contact any outside agencies needed.